

# **EXHIBIT 17**

**From:** Johnson, Rani [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=0EE57945F15E47B3ABAA99A59170AD3F-JOHNSON, RA]  
**Sent:** 9/20/2018 4:33:59 PM  
**To:** Mitchen, Joe [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=30560e8a83be4b49b188bee96965ed3e-Mitchen, Jo]; Carroll, Bill [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=797b1f3932174f7d989aee6bf00bd3d3-Carroll, Bi]  
**Subject:** FW: Please confirm (particularly the threat modeling) THIS ONE

---

**From:** Colquitt, Steven  
**Sent:** Monday, May 21, 2018 9:45 AM  
**To:** Brown, Timothy <[timothy.brown@solarwinds.com](mailto:timothy.brown@solarwinds.com)>; Johnson, Rani <[rani.johnson@solarwinds.com](mailto:rani.johnson@solarwinds.com)>  
**Subject:** RE: Please confirm (particularly the threat modeling)

I don't see a line item about threat modeling... but since you mentioned it.

TM'ing is a process. It's part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity. So I am not sure what you are looking for in terms of confirmation.

---

**From:** Brown, Timothy  
**Sent:** Monday, May 21, 2018 7:24 AM  
**To:** Johnson, Rani <[rani.johnson@solarwinds.com](mailto:rani.johnson@solarwinds.com)>  
**Cc:** Colquitt, Steven <[steven.colquitt@solarwinds.com](mailto:steven.colquitt@solarwinds.com)>  
**Subject:** RE: Please confirm (particularly the threat modeling)

I updated the table to call out Checkmarks as being implemented, I added Snyk to this section It is being used by the cloud team, I also added OpenVAS to the list of vulnerability scanners

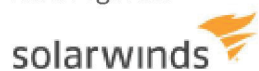
---

**From:** Johnson, Rani  
**Sent:** Monday, May 21, 2018 7:45 AM  
**To:** Brown, Timothy <[timothy.brown@solarwinds.com](mailto:timothy.brown@solarwinds.com)>  
**Cc:** Colquitt, Steven <[steven.colquitt@solarwinds.com](mailto:steven.colquitt@solarwinds.com)>  
**Subject:** Please confirm (particularly the threat modeling)

Security Capabilities	Tools
Vulnerability Assessment / Scanning	Rapid7 Nexpose Enterprise, OpenVAS
Endpoint Security	Symantec Endpoint Protection (SEP), SolarWinds-MSP Managed A/V (Bitdefender), Microsoft Bitlocker Full Disk Encryption (FDE)
Network Security	Palo Alto Next Generation Firewalls

<b>Security Information &amp; Event Management</b>	SolarWinds Log and Event Manager (LEM)
<b>Data Loss Prevention</b>	Netskope Cloud Security Access Broker (CASB), Helix Threat Detection
<b>Credential Management</b>	Thycotic Secret Server, Microsoft
<b>Access Control</b>	Palo Alto Global Protect VPN client, Active Directory
<b>Security Analytics</b>	Interset (behavior analysis)
<b>Email Security</b>	Cisco Ironport, Microsoft O365
<b>Code Analysis</b>	Tenable-Nessus, Black Duck, SonarQube, Cppcheck, Clang-Tidy, OpenVas, OWASP Zap Proxy Checkmarks-SASTcx, snyk
<b>PEN Testing</b>	Rapid 7 MetaSploit, Burp Suite, various PEN testing services
<b>Digital Forensic Toolkit</b>	Access Data FTK

Kind regards.



**Rani Johnson** | Chief Information Officer | **SolarWinds**

Office: 512.682.9541 | Mobile: 512.299.0610 | Wearable: 512.736.3400